We Claim:

1. A method for communicating confidential data from a sender to a receiver, comprising the steps of:

(A) encrypting the confidential data while the confidential data is in the control of the sender, said step of encrypting including mixing the confidential data with biometric data to produce encrypted data;

(B) sending the encrypted data over a communication link to the receiver;

(C) de-encrypting the encrypted data while the encrypted data is in the control of the receiver by separating the biometric data from the confidential data.

2. The method of Claim 1, wherein the biometric data includes first biometric data relating to the receiver and further including the steps of:

(D) isolating the first biometric data from the encrypted data after said step of sending;

(E) generating second biometric data relating to the receiver; and

(F) comparing the first biometric data to the second biometric data to determine if there is a predetermined level of similarity therebetween, said steps of isolating, generating and comparing being conducted prior to said step of de-encrypting, with the execution or non-execution of said step of de-encrypting being dependent upon whether the predetermined level of similarity is present.

3. The method of Claim 2, wherein said step (A) of encrypting includes mixing an additional data component with the confidential data and the first biometric data

to produce the encrypted data, the additional data component and the confidential data remaining mixed after said step (D) of isolating the first biometric data, said step (C) of de-encrypting including separating the confidential data from the additional data component.

4. The method of Claim 3, wherein the additional data component includes secret key data.

5. The method of Claim 4 wherein the secret key data is combined with the confidential data via a logical/mathematical operation to encrypt said confidential data.

6. The method of Claim 5, wherein the secret key data is combined with the confidential data before said step of mixing the confidential data with the biometric data in said step (A).

7. The method of Claim 6, wherein the secret key data is de-combined from the confidential data after said step of separating the biometric data from the confidential data in said step (C).

8. The method of Claim 7, wherein the secret key data is combined with the biometric data via a logical/mathematical operation to encrypt the biometric data and wherein the secret key data is de-combined from the biometric data after said step of separating the biometric data from the confidential data in said step (C).

9. The method of Claim 8, further including the step of deriving the secret key data from a password via a predefined logical/mathematical formula.

10. The method of Claim 5, wherein the secret key data is combined with the biometric data via a logical/mathematical operation to encrypt said biometric data.

11. The method of Claim 3, wherein the additional data component is third biometric data.

12. The method of Claim 11, wherein the third biometric data is a voice signature of the sender and further including the steps of:

(G) producing a reference voice signature for the sender; and

(H) storing the reference voice signature produced in step (G), prior to said step (A) of encrypting the confidential data.

13. The method of Claim 3, wherein the first biometric data is a reference voice signature of the receiver and further comprising the steps of:

(I) producing the reference voice signature for the receiver;

(J) storing the reference voice signature produced in step (I); and

(K) communicating the reference voice signature of the receiver to the sender prior to said step (A) of encrypting the confidential data.

14. The method of Claim 13, wherein the reference voice signature is stored on a server computer on the Internet and said step (K) of communicating includes downloading the reference voice signature from the server computer to a sender computer available to the sender.

15. The method of Claim 14, wherein the reference voice signature is stored on the server computer in association with a flag indicating the necessity of the receiver giving prior authorization to the sender before receiving confidential data from the sender; and further including the step of checking the status of the flag prior to downloading the reference voice signature.

16. The method of Claim 15, wherein said step (B) of sending includes uploading the encrypted data from the sender computer to the server computer; storing the encrypted data on an email system on the server computer; and downloading the encrypted data from the server computer to a receiver computer available to the receiver.

17. The method of Claim 16, wherein the encrypted data is stored on the receiver computer for a predetermined time and then deleted automatically.

18. The method of Claim 13, wherein said step (E) of generating includes deriving a voice signature from a speech sample given in real time by the receiver.

19. The method of Claim 18, wherein said step (E) of generating includes the receiver speaking into an audio input of a computer to provide a speech sample, the speech sample being processed by the computer to derive the voice signature.

20. The method of Claim 1, wherein the confidential data is in the form of a computer file residing on a first computer controlled by the sender, wherein the communication link is a computer network and said step of sending includes sending the encrypted data over the computer network to a second computer in the control of the receiver.

21. The method of Claim 20 further including the step of:

(L) converting the encrypted data from a first file format to a second file format before said step (B) of sending.

22. The method of Claim 21, wherein the second file format is a wave file format.

23. The method of Claim 21, wherein said step (C) of de-encrypting includes reconverting the second file format to the first file format.

24. The method of Claim 20, wherein the computer network includes the Internet and said step (B) of sending includes the transfer of the encrypted data from the first computer to a server computer and from the server computer to the second computer.

25. A method for encrypting and de-encrypting confidential data, comprising the steps of:

(A) Encrypting the confidential data by combining the confidential data with secret key data in accordance with a first predetermined logical/mathematical algorithm to produce data at a first level of encryption;

(B) Obtaining biometric data relating to a living creature;

(C) Mixing the biometric data with the data at the first level of encryption in accordance with a second predetermined algorithm to produce data at a second level of encryption;

(D) De-encrypting the data at the second level of encryption by separating the data at the second level of encryption with the biometric data and the data at the first level of encryption using the second pre-determined algorithm in reverse; and

(E) De-combining the confidential data and the secret key data using the reverse of the first predetermined logical/mathematical algorithm.

26. The method of Claim 25, further comprising the step of converting the data at the second level of encryption from a file of a first format to a file of a second format after said step (C) of mixing and wherein said step (D) of de-encrypting includes reconverting from the second format to the first format prior to said step of separating.

27. The method of Claim 26, wherein the second file format is a wave file format.

28. The method of Claim 27, wherein said step (B) of obtaining includes generating a speech sample and deriving a voice signature from the speech sample constituting the biometric data, and further including verifying the voice signature after said step of separating by generating a second speech sample and deriving a second voice signature and comparing the voice signature of the biometric data to the second voice signature to determine a predetermined degree of similarity prior to said step of de-combining.